REMARKS

In response to the Office Action mailed August 21, 2007, Applicant respectfully requests reconsideration. Claims 1-19, 25-33, and 44-51 were previously pending in this application. By this paper, claims 2, 25-26, 29, and 47 have been amended. No claims have been added or canceled. As a result, claims 1-19, 25-33, and 44-51 are pending for examination with claims 1, 10, 20, 25 and 47 being independent claims. No new matter has been added.

I. Summary of Telephone Conference with Examiner

First, Applicants' representative appreciates the courtesies extended by Examiner Gelagay in granting and conducting a telephone conference on November 13, 2007. Applicants were represented at the interview by Ed Walsh and Technology Specialist Andrew Tibbetts. During the telephone conference, Applicants' representative presented to the Examiner a general overview of Applicants' invention as recited in the claims. The Hassan reference was also discussed.

During that discussion, the Examiner indicated that she believed a passage in the Hassan reference, not mentioned in the Office Action, taught the methods sought to be claimed by Applicants. This passage is discussed below in the overview of the Hassan reference.

Further details of various topics discussed during the telephone conference with the Examiner are included in the remarks below.

II. Overview of Embodiments of the Invention

As an aid to the Examiner, Applicants provide below a summary of the specification of the present application. This summary is not intended as a substitute for the Examiner reading the application in its entirety, as all embodiments of the invention are not described below. Also, the summary is not intended to characterize the claims or terms used in the claims, which are discussed individually below.

Briefly, as illustrated by FIG. 8, the present application describes a process by which hosts exchange messages using any of a number of modulation schemes. The modulation schemes are illustrated in FIG. 8 by $M_1, M_2 \ldots M_n$. As illustrated in Table 1, the modulation schemes may encode different numbers of bits per symbol. Accordingly, because the messages

exchanged use different modulation schemes, different number of bits may be communicated in each message.

In the example of FIG. 8, the first message communicates a set of bits B_0. In subsequent messages, sets of bits B_1, B_2, ... B_n are communicated. In this way, once the messages are communicated both of the hosts have access to sets of bits B_0, B_1... B_n. These sets of bits are used to construct on each host a key, identified as K_1 in FIG. 8. Once the hosts have exchanged enough bits so that each can construct a key, the hosts may thereafter communicate securely using that key.

For effective communication, the host that receives a message decodes the message using the same modulation scheme that was used by the host to send the message. An unauthorized listener to this exchange of messages does not know the modulation scheme used in each message and therefore cannot readily determine the bits forming the key that are communicated in each message. Though the modulation schemes may be changed randomly from message-to-message to make it more difficult for an unauthorized listener to guess the bits communicated in each message, each host knows which modulation scheme to use for each message it receives and can readily determine the bits that are used to form the key. Each host knows the modulation schemes of each message because each time a host communicates a set of bits, it also instructs the other host on which modulation scheme to use in a subsequent message.

For example, as illustrated in FIG. 8, when host A transmits a set of bits B_0, it also transmits an indication that modulation scheme M_1 should be used for a subsequent message. Accordingly, when host B sends a set of bits B_1, it encodes those bits using modulation scheme M_1. Along with the communication of bits B_1, host B sends to host A, including an indication that modulation scheme M_2 should be used for a subsequent communication. The process may continue in this fashion iteratively until a sufficient number of bits is communicated between host A and host B.

The foregoing summary is provided solely for the convenience of the Examiner. It should be appreciated that each of the independent claims may not be limited in the manner described in the summary above. Therefore, the Examiner is requested not to rely upon the summary for determining whether each of the claims distinguishes over the prior art of record, but to do so based solely on the language of the claims themselves.

III. Rejections under 35 U.S.C. §112

Claims 2 and 26 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicants have herein amended claims 2 and 26. Accordingly, withdrawal of the rejection of claim 2 and 26 under 35 U.S.C. §112 is respectfully requested.

IV. Claim Rejections Under 35 U.S.C. §103

Claims 1-4, 10-15, 19, 25-28 and 44-51 stand rejected under 35 U.S.C. 103(a) as allegedly being obvious over U.S. Patent No. 6,031,913 ("Hassan") in view of Published U.S. Application No. 2004/0091054 ("Rastegar"). Having amended claim 25 purely to clarify further Applicants' contributions to the art, and claim 47 merely to correct a grammatical error, Applicants respectfully traverse the rejection.

A. Overview of Hassan

Applicants understand Hassan to teach methods for using "characteristics of a communication channel" to "establish key sequences for use in encrypting communicated information" (Hassan, Abstract). These characteristics of the communication channel may be, for example, an impedance of the communication channel as viewed from one transceiver to the other and vice versa. To determine an impedance of a communication channel, a plurality of tones are transmitted from a first transceiver to a second transceiver, with each tone having a predetermined frequency and initial phase (Col. 3, lines 31-33). The second transceiver, upon receiving the tones, transmits the received tones back through the communication channel "without substantial change," simply acting as a repeater for the signal. (Col. 7, lines 7-10). The first transceiver, upon receiving the re-transmitted tones, analyzes the received tones and compares them to the tones originally transmitted to calculate differences in phase and magnitude. The series of transmissions (of tones or bits) and calculations described above is carried out a second time with the second transceiver transmitting first (Col. 3, lines 37-44).

In both transceivers, then, the calculated differences are "quantized … into a respective one of a plurality of phase decision values" and an encryption key is determined according to a predetermined block code (Col. 3, lines 45-63). Thus, the exact tones exchanged by the transceivers are irrelevant to the encryption key determined by the method, but rather only serve

as a signal from which the method may determine characteristics of the communication channel. Hassan further teaches that it is important for these transmissions, re-transmissions, and calculations to occur quickly because the impedance of a communication channel may not appear to be the same in both directions except "when considered on a short time scale" (Col. 6, lines 10-27).

In an alternative embodiment, to which the Examiner referred in the Telephone Interview, Hassan teaches that rather than transmitting tones, a series of bits (e.g., pilot symbols) may be transmitted, such as the bits that may be transmitted for synchronizing the operation of a first transceiver and a second transceiver (i.e., pilot symbols) (Col. 10, lines 49-54). Bits received at a host may be mapped to the center of a sphere to yield a key, or may be compared to predetermined bits to calculate "differences between each of the estimates [for the bits] and the respective predetermined bits" such as differences in phase (Col. 10, lines 56-57; col. 11, lines 13-30). These differences are then used, just as the differences in tones above, to determine characteristics of the network over which the bits were transmitted, and these characteristics may then be used to determine an encryption key (Col. 11, lines 20-30). Thus, the actual bits transmitted are irrelevant to the encryption key determined by the method, but rather only serve as a signal from which the method may determine characteristics of the communication channel.

B. Overview of Rastegar

Rastegar teaches methods for performing "low-detectability communication between a transmitter and receiver" (Rastegar, Abstract). Rastegar teaches that a transmitter, such as a sensor, may need to transmit information wirelessly in such a way as to avoid detection (¶0005). To do so, when transmitting data, a sensor varies the timing, modulation, and frequency of its transmissions (¶0012). When varying the timing, modulation, and/or frequency, the transmitter, prior to varying the timing, modulation, and/or frequency, appends to a transmission information regarding the variation (¶0011). A receiver may then receive the information regarding the variation and reconfigure itself to receive transmitted data appropriately. Rastegar does not teach any methods for transmitting data to the sensor/transmitter (i.e., receiving data at the sensor/transmitter) but only transmitting data by the sensor/transmitter. Rastegar further describes that "the issue here is not the sensor data security (for which encryption is the appropriate tool), but about the detectability of the sensor itself," and therefore does not teach

methods of encryption (¶0006).

C. Claim 1 and its Dependents

Independent claim 1 is directed to a method of wirelessly generating a cryptographic key that may be used to encrypt wireless communications between a first host and a second host. The method comprises selecting an initial modulation scheme for wireless transmission between the first host and the second host. The method further comprises transmitting via the initial modulation scheme first data to be used in generating the cryptographic key and an indication of a second modulation scheme and receiving via the second modulation scheme second data to be used in generating the cryptographic key. The method additionally comprises generating the cryptographic key using the first and the second data.

The combination of Hassan and Rastegar does not teach or suggest all limitations of claim 1. For example, claim 1 recites transmitting first data and receiving second data to be used in generating a cryptographic key, and "generating a cryptographic key using the first and the second data." As described above, in the system of Hassan two hosts exchange tones or bits as part of a process for generating a cryptographic key. These tones/bits, however, are not used to generate a cryptographic key. Rather, the tones/bits of Hassan are merely transmitted and relayed to determine characteristics of the network over which the tones/bits are being transmitted (e.g., impedance) by analyzing, for example, a phase shift in the tones/bits. It is these determined characteristics of the network which are used by Hassan's method to generate a cryptographic key, and not the tones/bits. The data exchanged is irrelevant to the process of generating a cryptographic key.

Further, even if it could be said that Hassan teaches generating a cryptographic key from the tones/bits exchanged—which is clearly not the case—there is no teaching or suggestion in Hassan of using a first and second modulation scheme to communicate the first and second data. At best, Hassan teaches only transmitting to a second host first data (whether tones or bits) and receiving the first data back from the second host. The second host relays the first data "on a short time scale" and does so "simply" and "without substantial change" (Hassan, col. 6, line 17-18; col. 7, lines 8-9). Thus, the second host transmits the data back in the same modulation scheme, as modifying the modulation scheme would extend the time scale and would comprise a "substantial change" in the signal. There is no discussion in Hassan in transmitting data

(tones/bits) via a first modulation scheme and receiving data via a second modulation scheme. Any act of modifying the data at the second host to change the modulation scheme would run counter to the teachings of Hassan and render Hassan unfit for its intended purpose. Because the encryption key of Hassan is determined from the characteristics of the network, and the characteristics of the network are determined from changes in the exchanged data, the hosts of Hassan should be adapted to minimize their own impacts on the signal such that the changes to the signal are only those imposed by the network. Any substantial changes to the signal, such as those that would be made by the second host when changing a modulation scheme of the signal, would inevitably impact the signal in ways that could not be attributed to the network (e.g., the host would change the phase of the signal). Therefore, the first host, upon receiving the relayed data, could not determine accurately the characteristics of the network, because the signal would have been modified substantially in ways that could not be attributed to the network. Modifying a modulation scheme of the signal would, therefore, impede the first host's ability to determine characteristics of the network and therefore also impede the ability to generate an encryption key based on those characteristics.

Modifying Hassan with the teachings of Rastegar would not cure these deficiencies of Hassan. First, one of ordinary skill in the art would not have been compelled to combine Hassan or Rastegar in any manner, or modify the teachings of Hassan with the teachings of Rastegar in any manner, because the references are directed to solving different problems in different ways. While Hassan teaches methods for "establishing key sequences for use in encrypting communicated information," Rastegar explicitly states that "the issue here is *not the sensor data security* (for which encryption is the appropriate tool), but about the detectability of the sensor itself" (Hassan, Abstract; Rastegar, ¶0006) (emphasis added). One of ordinary skill in the art seeking to expand on the encryption methods of Hassan would thus not have looked to Rastegar because Rastegar does not provide any teaching or suggestion on how to improve methods for establishing encryption key sequences or, indeed, any encryption method. Therefore, no combination of Hassan and Rastegar would lead to the method of claim 1 because no such combination is desirable or feasible.

Further, even if Hassan and Rastegar were combined, the combination would not meet all limitations of claim 1. First, it should be apparent that because Rastegar, by its own explicit admission, does not teach any method involving encryption, it cannot teach an act of "generating

a cryptographic key using first and second data" or "transmitting ... first data to be used in generating the cryptographic key." Second, as described above, Rastegar teaches methods for controlling a sensor to transmit data when the sensor is "in a location which is inaccessible to the user after deployment" (¶0005). Thus, because the sensors cannot be interacted with or communicated with after deployment (because they are "inaccessible"), Rastegar teaches only methods for *transmitting* data from a sensor using varying modulation schemes using varying modulation schemes. Nowhere does Rastegar teach or suggest an act of receiving any data, let alone receiving data via a second modulation scheme. Thus, Rastegar cannot teach or suggest "receiving via the second modulation scheme second data to be used in generated the cryptographic key," as recited by claim 1.

Additionally, as discussed above, modifying Hassan in any way to include the varying modulation schemes taught by Rastegar would render Hassan unfit for its intended purpose. Because the encryption key of Hassan is determined from the characteristics of the network, and the characteristics of the network are determined from changes in the exchanged data, the hosts of Hassan should be adapted to minimize their own impacts on the signal such that the changes to the signal are only those imposed by the network. Any substantial changes to the signal, such as those that would be made by the second host when changing a modulation scheme of the signal, would inevitably impact the signal in ways that could not be attributed to the network (e.g., the host would change the phase of the signal), and thus impede the first host's ability to determine characteristics of the network and generate an encryption key based on those characteristics.

At best, then, any combination of Hassan and Rastegar would require further modifications to the combination not taught by either reference to teach fully the method recited by claim 1.

Therefore, for at least these reasons, claim 1 patentably distinguishes over any combination of Hassan and Rastegar and is in allowable condition. Claims 2-9 and 44-45 depend from claim 1 and are allowable for at least the same reasons.

D. Claim 10 and its Dependents

Independent claim 10 is directed to a method of wirelessly generating a cryptographic key that may be used to encrypt wireless communications between a first host and a second host.

The method comprises transmitting data between the first host and the second host using varying modulation schemes for each transmission, and generating the cryptographic key from the data.

For reasons that should be appreciated from the foregoing discussion of independent claim 1, one of ordinary skill in the art would not have had a reason to combine Hassan and Rastegar in any manner, nor does the combination of Hassan and Rastegar teach or suggest all limitations of claim 10. For example, neither Hassan nor Rastegar teaches or suggests "generating a cryptographic key" from data "transmitted between a first host and a second host using varying modulation schemes for each transmission." Hassan, for its part, teaches generating a cryptographic key based on conditions and characteristics of a network which may be determined from tones or bits transmitted through the network (e.g., an impedance of the network may be determined from a phase shift introduced by the network into the tone/bit signal). In Hassan, the data transmitted is not relevant to determining a cryptographic key, but rather the cryptographic key is generated based on the detected characteristics of the network. Rastegar does not teach any act of generating a cryptographic key, as it explicitly states that it is not directed to encryption/cryptography (¶0006).

Therefore, for at least these reasons, claim 10 patentably distinguishes any combination of Hassan and Rastegar and is in allowable condition. Claims 11-19 depend from claim 10 and are allowable for at least the same reasons.

E. Claim 25 and its Dependents

Independent claim 25, as amended, is directed to a computer storage medium having computer-executable instructions. The computer-executable instructions, when executed, perform steps comprising selecting an initial modulation scheme for wireless transmission between a first host and a second host ***and transmitting an initial value providing an index to the initial modulation scheme***. The method further comprises transmitting via the initial modulation scheme first data to be used in generating a cryptographic key and an indication of a second modulation scheme and receiving via the second modulation scheme second data to be used in generating the cryptographic key. Additionally, the method comprises ***generating the cryptographic key using the first and the second data***.

The combination of Hassan and Rastegar does not teach or suggest all limitations of amended claim 25. For reasons that should be appreciated from the foregoing discussion of claim

1, one of ordinary skill in the art would not have had any reason to combine Hassan and Rastegar, as any such combination is not desirable or feasible. Moreover, even if one of ordinary skill in the art would have combined the references, any such combination would not yield a method such as the one recited in claim 25. For example, neither Hassan nor Rastegar teaches or suggests transmitting first data and receiving second data to be used in generating a cryptographic key, and "generating a cryptographic key using the first and the second data."

Further, neither Hassan nor Rastegar teaches or suggests "transmitting an initial value providing an index to the initial modulation scheme." Hassan, for its part, does not teach or suggest any act of transmitting an index to an initial modulation scheme. In Hassan, the data exchanged between hosts prior to determining an encryption key is not processed by the hosts, but merely received and relayed, and thus there is no reason to exchange between the hosts an indication of a modulation scheme used to generate the exchanged signal. Even when the signal exchanged comprises bits, Hassan does not teach or suggest transmitting an initial value providing an index to an initial modulation scheme, but rather teaches only that the bits exchanged may be "known" by both hosts or "predetermined" (Hassan, col. 11, lines 25-27).

Rastegar does not cure the deficiencies of Hassan. In Rastegar, which does vary its modulation scheme, "initially, transmission times, frequency bands, and modulation keys are assumed to be selected sequentially by an algorithm that is known to both the sensor (transmitter) and receiver" (Rastegar, ¶0031). In Rastegar, then, no "initial value providing an index to an initial modulation scheme" is transmitted, because the modulation schemes are selected, at least at first, by an algorithm known to both the transmitter and the receiver. There is no reason in the system of Rastegar to transmit an initial value providing an index to an initial modulation scheme because both hosts are already aware of what the initial modulation scheme is by virtue of knowing in advance the algorithm which is used to select the initial modulation scheme. Thus, Rastegar does not teach or suggest any act of "transmitting an initial value, the initial value providing an index to an initial modulation scheme."

Therefore, for at least these reasons, claim 25 patentably distinguishes any combination of Hassan and Rastegar and is in allowable condition. Claims 26-33 depend from claim 25 and are allowable for at least the same reasons.

F. Claim 47 and its Dependents

Independent claim 47 is directed to a method of wirelessly generating a cryptographic key that may be used to encrypt wireless communications between a first host and a second host. The first host and the second host comprise a wireless interface supporting communication using a plurality of modulation schemes, ***where each modulation scheme of the plurality of modulation schemes encodes a number of bits per symbol with the number of bits being different for different modulation schemes of the plurality of modulation schemes***. The method comprises, for each of a plurality of iterations, communicating a message between the first host and the second host using a modulation scheme. The message communicates a set of bits and a subsequent modulation scheme. ***The number of bits in the set of bits is based on the number of bits per symbol of the modulation scheme.*** For each iteration after the first iteration, the modulation scheme is identified in a message communicated in a prior iteration. The method further comprises generating the cryptographic key using the sets of bits communicated in the plurality of iterations.

For reasons that should be appreciated from the foregoing discussion of claim 1, the combination of Hassan and Rastegar does not teach or suggest all limitations of claim 47. As discussed above, Hassan does not teach or suggest any act of varying modulation schemes, and thus does not teach or suggest an act of communicating a set of bits where the number of bits in the set of bits is based on the number of bits per symbol of the modulation scheme. Further, when transmitting bits (rather than tones), Hassan suggests that the number of bits transmitted may be related to the network over which the bits are transmitted, and not the modulation schemes used to transmit the bits over the network: "If the pilot symbols were the sync bits in a cellular radio telephone system, it is currently believed that at least sixty bits would be needed" (Col. 11, lines 1-3). Hassan, then, does not teach communicating a set of bits where the number of bits in the set of bits is based on the number of bits per symbol of the modulation scheme.

Rastegar, for its part, teaches varying modulation schemes, but does not teach or suggest relating the content of a message (i.e., the number of bits in the message) to the modulation scheme. Rastegar describes that "we assume that the data are to be transmitted in a digital format consisting of several words, each of which has a number of binary digits … the transmitter can encode information into each word about changes in the timing, frequency, or modulation of the next word to be transmitted" (Rastegar, ¶0031). Rastegar does not teach or suggest varying an

amount of data transmitted as a modulation scheme is varied, but instead only teaches transmitting "several words" along with "information ... about changes" to the modulation scheme. Rastegar, then, does not teach communicating a set of bits where the number of bits in the set of bits is based on the number of bits per symbol of the modulation scheme.

Therefore, for at least these reasons, claim 47 patentably distinguishes over any combination of Hassan and Rastegar and is in allowable condition. Claims 48-51 depend from claim 47 and are allowable for at least the same reasons.

CONCLUSION

In view of the foregoing amendments and remarks, this application should now be in condition for allowance. A notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicants' representative at the telephone number indicated below to discuss any outstanding issues relating to the allowability of the application.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicants hereby request any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Dated: November 21, 2007

Respectfully submitted,

By: /Edmund J. Walsh/

Edmund J. Walsh
Registration No. 32,950
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, Massachusetts 02210-2206
Telephone: (617) 646-8000